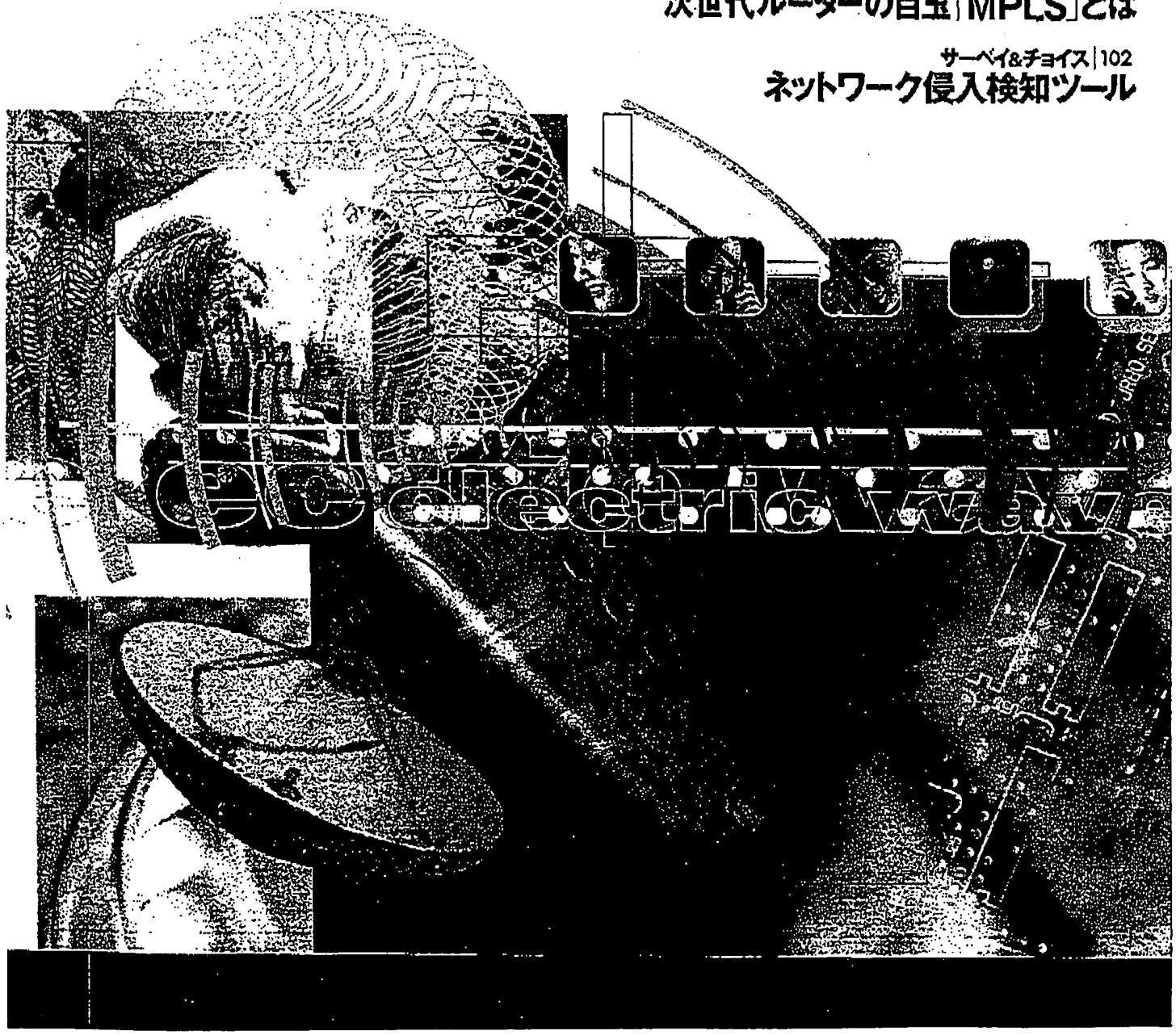
日経コミュニケーション

NIKKEI COMMUNICATIONS Citation 1

10/18
1999

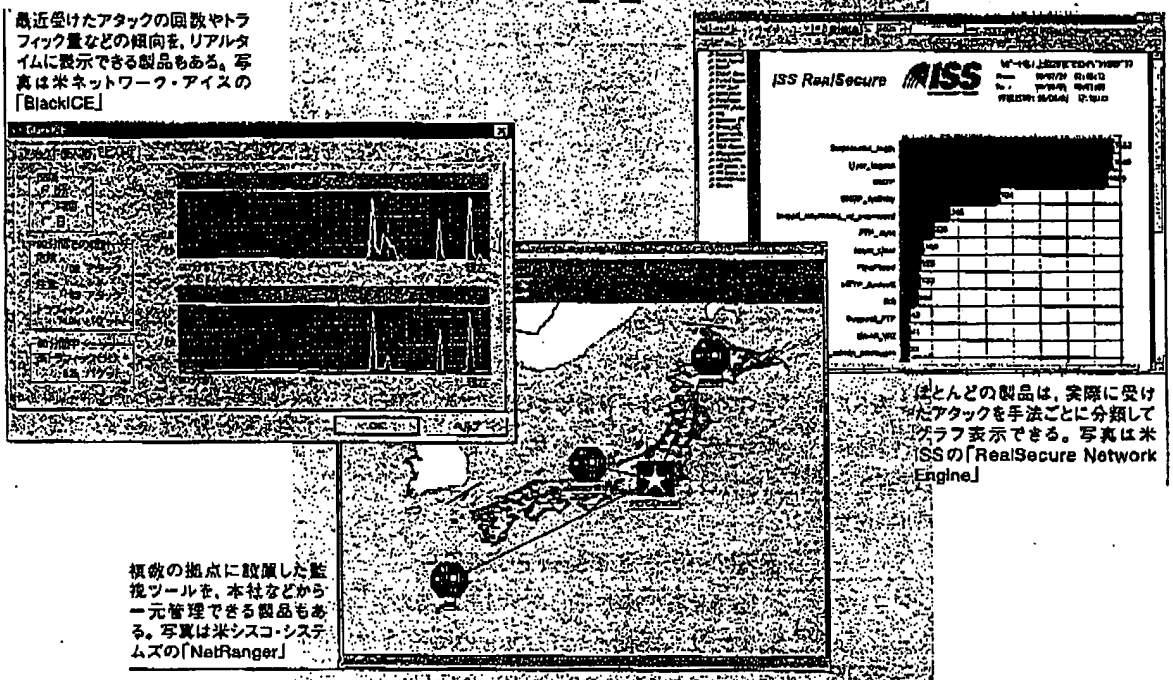


不正アクセス
セキュリティ
ネットワーク管理

Citation 1

(ネットワーク侵入検知ツール)

不正アクセスを監視，撃退 犯人発見の精度を競う



最近受けたアタックの回数やトラフィック量などの傾向を，リアルタイムに表示できる製品もある。写真は米ネットワーク・アイスの「BlackICE」

ほとんどの製品は，実際に受けたアタックを手法ごとに分類してグラフ表示できる。写真は米ISSの「RealSecure Network Engine」

複数の拠点に設置した監視ツールを，本社などから一元管理できる製品もある。写真は米シスコ・システムズの「NetRanger」

侵入検知ツールは，社内ネットワーク上の通信を監視して不正アクセスを防ぐためのソフトウエアである。99年10月現在，国内で入手可能な主なものは9製品にのぼる。とくに99年以降，新製品が続々と登場している。

不正アクセス対策には，ファイアウォールやサーバーのログの定期的なチェックが欠かせない。しかし現実には，ログを毎日チェックするのは大変な作業。管理者が専任でない場合はなおさらである。事実，本誌が98年に実施した調査では，上場企業中心の約800社のうち，毎日ログをチェックしていると回答した企業は3割にも満たない(98年11月2日号参照)。

侵入検知ツールは，こうした管理者の負担を減らすための監視カメラ的なツールである。「IDS」(intrusion detection system：侵入検知システム)とも呼ばれる。ネットワークやサーバーを24時間リアルタイムに監視して，問題があれば管理者に報告してくれる。また，ほとんどの製品は，不正アクセスの検知だけでなく，☞TCPコネクションを強制切断するなど防御も自動的にしてくれる。ただし，侵入検知ツールはすべての不正アクセスを発見してくれるツールではない。当然，限界もある。

Citation 1

本文中☞の付いた用語を解説

TCP = transmission control protocol。2種類あるIPの上位プロトコルのうちの一つ。RFC793で規定。もう一つのUDPに比べ，信頼性の高い通信を実現できる。

セグメント＝LANの構成単位。通常はリピータで区切られた範囲である。広義にはコリジョン・ドメインやブロードキャスト・ドメインを指すこともある。

クラッカ＝cracker。ネットワーク経由で他人のコンピュータ・システムに不正にアクセスしたり，攻撃を仕掛けるユーザー。

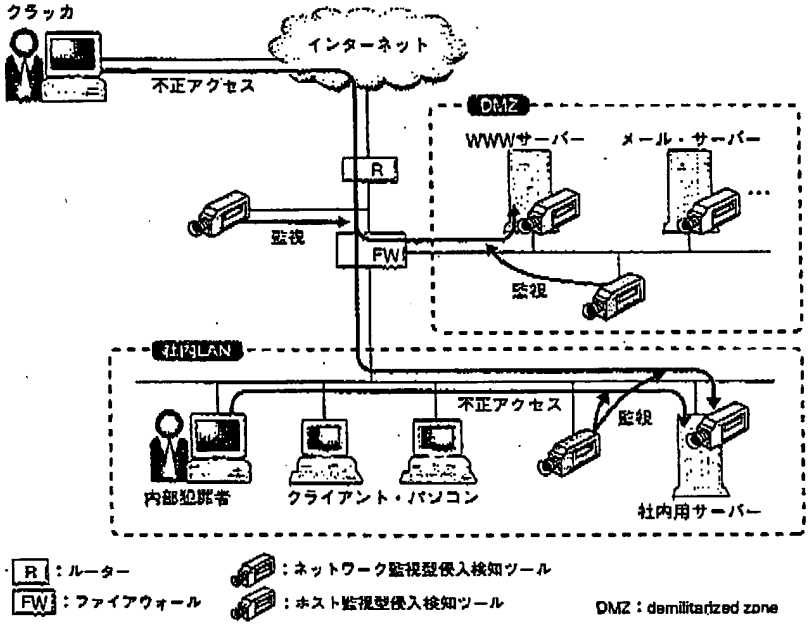
ポート・スキャン＝不正アクセスの一種。TCP/UDPのポートに順番にアクセスして，サーバーで稼働しているサービスを調べる行為。クラッカが不正アクセスの前段階として実行する。

国内でも製品開発が始まる

ベンダー各社によれば，現状では侵入検知ツールのユーザーは，大手メーカーの設計/研究部門や金融機関など，重要な電子データを扱う企業が中心だという。しかし各社とも今後は，電子商取引などの発展にともなって，一般の企業ユーザーの導入が確実に増えると見ている。

現在出荷されている侵入検知ツールはすべて海外ベンダーの製品である。ただ，国内でも開発の動きが出始めている。徳島大学の森井昌克教授らのグループや情報処理振興事業協会（IPA）は，国内ベンダーと協力して侵入検知ツールを開発中である。そのほか，電気通信大学の高田哲司氏らのグループもログを可視化して不正アクセスの検知を可能にするソフトを開発している。

図1 侵入検知ツールの概要 ネットワーク上を流れるパケットを監視する「ネットワーク監視型」とサーバーなどホスト・マシン上でユーザーの挙動を監視する「ホスト監視型」の2種類に大きく分けられる。前者は主に，パケットの内容を見て不正アクセスを調べる。一方後者は，主に対象となるサーバー上でのユーザーの行動を監視する。



パケットや挙動で不審者をチェック

一般に侵入検知ツールは，☞セグメント上を流れるすべてのパケットを監視する「ネットワーク監視型」と，重要なデータが置かれたファイル・サーバーなど特定のマシン上でユーザーの挙動を監視する「ホスト監視型」の2種類に大きく分けられる（図1）。

一般的な構成としては，ネットワーク監視型の場合は「センサー」などと呼ばれる専用マシン，ホスト監視型の場合は「エージェント」と呼ばれる監視プログラムをそれぞれ監視対象セグメントやサーバーに導入する。さらに，センサーやエージェントからの情報を受け取り，管理者が集中管理するための「コンソール」端末を設置する。

ネットワーク監視型の製品は，米ISSの「RealSecure Network Engine」（以下，RealSecure N/E）や米シスコ・システムズの「NetRanger」などが代表的だ。

一方ホスト監視型の製品には，米アクセント・テクノロジーズの「Intruder Alert」や米RSAセキュリティの「Kane Security Monitor」などがある。

ネットワーク監視型とホスト監視型の2種類があるのは，それぞれ得手不得手があり，どちらか一方では多種多様な不正アクセスの手法に対応しきれないからである。

基本的にネットワーク監視型は，パケットのヘッダーやデータ部分を見て正当性を判断する。このため，☞クラッカなどが不正アクセスの前段階として利用する☞ポート・スキャンや☞DoS攻撃などは簡単に発見できる。しかし，クラッカが事前に何らかの方法でID/パスワードを入手して，正規のユーザーになりすましている場合などには，ネットワーク監視型では発見は難しい。

一方，ユーザーの挙動を見るホスト監視型は，たとえ正規のユーザーであっても，例えばシステム・ファイルを勝手に書き換えようとするなどの不審な行動をとれば不正アクセスと判断で

DoS = denial of service．インターネットを経由した不正アクセスの一つ．システムのサービスを停止させたり，システム自体を停止，再起動させる攻撃である．ping of deathなどが代表的．

LANアナライザ＝LANの性能監視，障害解析などに利用する装置またはソフトウエア．プロトコル・アナライザとも呼ぶ．LAN上を流れるフレームやパケットを収集，加工，表示する機能を持つ．

きる。逆にホスト監視型は，ポート・スキャンやDoS攻撃など，パケット・レベルの不正アクセスには基本的には対処できない。

200以上の「指紋」が決め手

侵入検知ツールの仕組みを詳しく見ていこう。

まずはネットワーク監視型から。検知の基本的な流れは，①パケットの収集，②攻撃手法データベースとのパターン・マッチング，③管理者への警告と攻撃への対処――となる。

①のパケットの収集には，パソコンに装着されたNIC（network interface card）を，すべてのパケットを収集する「プロミスキャス・モード」（無選別モード）と呼ぶ特別な状態で利用する。基本的にはLANアナライザと同じ仕組みである。

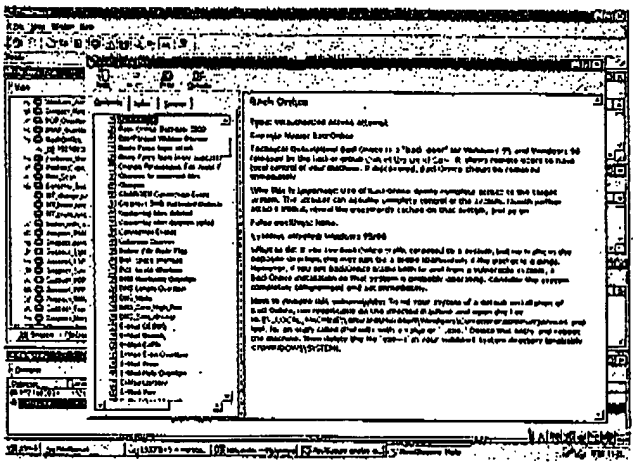


写真1　ネットワーク監視型侵入検知ツールはシグネチャと呼ばれる攻撃手法データベースを基に攻撃を発見する　写真は米ISSの「RealSecure Network Engine」のシグネチャ・リスト。個々の攻撃手法の詳細な説明が見られる。

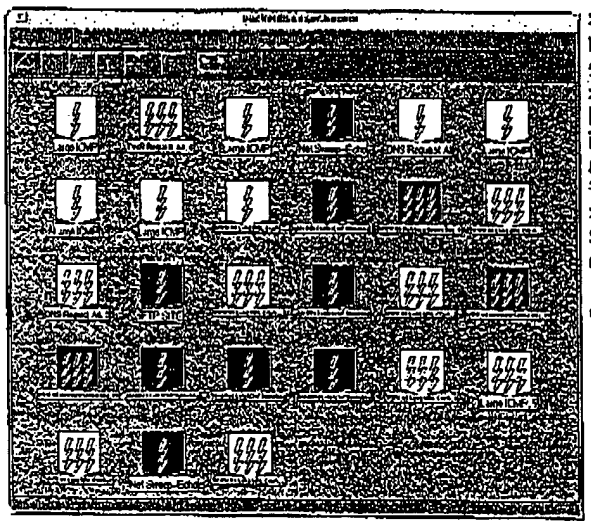


写真2　管理者のコンソール画面への警告表示が侵入検知時の基本的動作　写真は米シスコ・システムズの「NetRanger」のコンソール画面。攻撃を3段階の危険度で表示する。管理者への警告は，コンソールへの表示のほかに電子メールやSNMP（simple network management protocol）トラップでの通知に対応する製品が多い。

収集したパケットは直ちに，②の攻撃手法データベースとのパターン・マッチングにかけられる。データベースは，既存の不正アクセス手法の特徴を「シグネチャ」として格納してある。シグネチャとは，犯人が現場に残す指紋のようなものだ（写真1）。

シグネチャの数は製品ごとに異なるが，似たような攻撃手法を一つのシグネチャと数えるか，すべて別のシグネチャとするかなど定義の仕方が異なるため，単純な比較はほとんど意味がない。多くの製品は，200以上の攻撃手法に対応しており，著名な攻撃手法はほとんど検出できる。

パターン・マッチングの結果不正アクセスと判断した場合には，管理者へのアラート（警告）や，可能であればTCPコネクションの強制切断などの防御処理が施される（写真2）。

ホスト監視型も基本的な検知の流れはネットワーク監視型と同じである。①でパケットの代わりにサーバー上のログを監視する。同様に②では，ログとユーザーのファイル・アクセス権限や許可する行動などの規則（ルール）を組み合わせた「ポリシー」を，パターン・マッチングで比較して不正アクセスを検知する。

DoS攻撃には通信経路をしゃ断

次に，基本機能以外の付加機能を見てみよう。製品ごとの特徴が大きく表れる部分である。

まずは，ルーターやファイアウォールとの連係機能。ほとんどの製品は，

Citation 1

表1 国内で入手可能な主な侵入検知ツール シグネチャの数やルールの数え方は、ベンダーによって大きく異なる。

製品名	NetProwler	NetRanger	RealSecure Network Engine	BlackICE (Sentry/pro)	SessionWall-3
動作形態	ネットワーク監視型	ネットワーク監視型	ネットワーク監視型	ネットワーク監視型	ネットワーク監視型
開発	米アクセント・テクノロジーズ	米シスコ・システムズ	米ISS	米ネットワーク・アイス	米コンピュータ・アソシエイツ
国内販売元(問い合わせ先)	日新電機(☎03-5821-5914)	日本シスコシステムズ(☎03-3342-4100) *1	アイ・エス・エス(☎03-5475-6453)	京陽テクニカ(☎03-3279-0771)	コンピュータ・アソシエイツ(☎0120-702600) *2
シグネチャあるいはルールの数	158	約200	187	約300	117
アラートの通知方法(管理コンソールへの表示以外)	電子メール、ページャ、SNMPトラップ、ユーザー・コマンドの実行など	電子メール、SNMPトラップ、ユーザー・コマンドの実行など	電子メール、SNMPトラップ、ユーザー・コマンドの実行など	電子メール、ページャ、SNMPトラップなど	電子メール、FAX、SNMPトラップ、ユーザー・コマンドの実行など
ルーターやファイアウォールとの連係	ファイアウォール	ルーター	ファイアウォール、ルーター*4	× (対応予定)	ファイアウォール、ルーター
監視対象(プロトコルやユーザーの行動)	71のプロトコル/サービス	0～1023番のTCP/UDPポート	数十のプロトコル/サービス	数十のプロトコル/サービス	178のプロトコル/サービス
ユーザーによる監視対象の定義(URLなど)	○	○	○	○	○
ステルス・モードの利用可否(ネットワーク監視型の場合)	○	○	○	○	○
日本語リポートの作成の可否	×	×*3	○	○	○
動作OS	WindowsNT	Solaris	WindowsNT、Solaris、Linux	Windows95/98/NT	WindowsNT
最小構成時の価格	110万円から	473万6000円から*5	1デバイス107万9000円から	125デバイスで187万4000円から	25ユーザー版が39万円から*6
国内出荷時期	99年7月	98年1月	97年5月	98年9月	98年10月
備考	上記価格には、ホスト監視型の「Intruder Alert」が1ライセンス含まれる	上記価格には米サン・マイクロシステムズ製ワークステーションの価格などが含まれる	オプションでHP OpenViewとの連係が可能	「BlackICE pro」は個々のマシン上で分散して動作するネットワーク監視型	ウイルス・チェックやURLフィルタリング機能なども備える

製品名	CyberCop Monitor	Intruder Alert	RealSecure System Agent	Kane Security Monitor
動作形態	ホスト監視型*7	ホスト監視型	ホスト監視型	ホスト監視型
開発	米ネットワーク・アソシエイツ	米アクセント・テクノロジーズ	米ISS	米RSAセキュリティ
国内販売元(問い合わせ先)	ネットワーク アソシエイツ(☎03-5408-0701)	日新電機(☎03-5821-5914)	アイ・エス・エス(☎03-5475-6453)	セキュリティ・ダイナミックス(☎03-3539-7667)
シグネチャあるいはルールの数	168	約300	182	約20
アラートの通知方法(管理コンソールへの表示以外)	電子メール、SNMPトラップ、ユーザー・コマンドの実行など	電子メール、ページャ、ユーザー・コマンドの実行など	電子メール、SNMPトラップ、ユーザー・コマンドの実行など	電子メール
ルーターやファイアウォールとの連係	× (年内出荷予定の次バージョンで対応)	×	ファイアウォール、ルーター*4	×
監視対象(プロトコルやユーザーの行動)	プロトコル/サービスやユーザーの行動など合計で168	ログインの失敗、ファイル操作、管理者権限の乱用など	ログインの失敗、ファイル操作、管理者権限の乱用など	ログインの失敗、ファイル操作、管理者権限の乱用など
ユーザーによる監視対象の定義(URLなど)	○	○	○	×
ステルス・モードの利用可否(ネットワーク監視型の場合)	○	—	—	—
日本語リポートの作成可否	×	×	○	○
動作OS	WindowsNT、Solaris、HP-UX(対応予定)	WindowsNT、SunOS、NetWare、IRIX、HP-UX、AIXなど	WindowsNT、Solaris	WindowsNT
最小構成時の価格	26デバイスで25万4800円/年から	マネージャ(管理コンソール)が50万円から、エージェントが2万円から	1デバイス19万4000円から	1サーバー・ライセンスが29万8000円から
国内出荷時期	98年10月	99年4月	99年1月	98年6月
備考				

*1 国内ではヒューコム(☎03-5308-7382)が主に販売 *2 ヒューコムがオプションで提供するツールを利用すれば作成可能 *3 ヒューコムの販売価格 *4 サポート外だが、付属プログラムを利用すればルーターと連係可能 *5 国内ではアズジェント(☎03-5643-2561)、フォーバルクリエーティブ(☎03-5466-3560)、オービックビジネスコンサルタント(☎03-5330-6550)が販売 *6 アズジェントの販売価格 *7 ネットワーク監視型の機能も備える(自分あてのパケットのみ)

telnet＝ネットワーク経由でほかのコンピュータに接続して遠隔操作を実現する仮想端末機能。TCPの上位アプリケーションであり，RFC854で規定。文字単位で通信する。ポート番号23番を利用。

FTP＝file transfer protocol。インターネット上の2点間でファイル転送するためのプロトコル。RFC959で規定。ポート番号20番と21番を利用。

UDP＝user datagram protocol。2種類あるIPの上位プロトコルのうちの一つ。RFC768で規定。TCPに比べると，処理負荷は軽いが，通信の信頼性は劣る。

不正アクセスを検知するとTCPコネクションの切断やサーバー上のプロセスの強制終了などが可能だ。しかし，これだけでは不十分である。切断しても繰り返し攻撃してくる可能性は十分ある。また，telnetやFTPなどTCPを利用した通信に関してはコネクションの強制切断が可能だが，ホスト間で送達確認をせず，一方的にパケットを送りつけるUDPを使ったDoS攻撃などは防げない。

こうした攻撃に対しては，上流にあるルーターやファイアウォールでパケットをフィルタリングする必要がある(図2)。

ルーターとの連係機能を備えた製品で代表的なのがシスコのNetRanger。同社製ルーターと連係が可能だ。具体的には，不正アクセス元からのパケットをすべてしゃ断するようにルーターのアクセス・コントロール・リスト(ACL)を書き換えられる。

以前はシスコ製ルーターと連係可能な製品はNetRangerだけだったが，最近では米コンピュータ・アソシエイツのSessionWall-3などほかのベンダーでも対応している製品がある。

ファイアウォールとの連係は慎重に

多くの侵入検知ツールは，ファイアウォールとの連係も可能だ。ルーターと同様に，不正アクセス元のIPアドレスからの通信をしゃ断するようにファイアウォールの設定を変更できる。

ほとんどのツールが連係可能なファイアウォールは，イスラエルのチェック・ポイント・ソフトウエア・テクノロジーズの「FireWall-1」。制御にはFireWall-1の標準API（application programming interface）である「OPSEC」を利用する。ほかにもOPSECに対応したファイアウォールであれば基本的に連係ができる。

ネットワーク・アソシエイツのCyberCop Monitorは，年内に出荷予定の次バージョンで同社製ファイアウォール「Gauntlet」と連係できるようにする。CyberCop Monitorは，「イベント・オーケストレータ」と呼ぶポリシー・サーバーを中心にしたポリシー・ベースの連係ができるのが大きな特徴である。

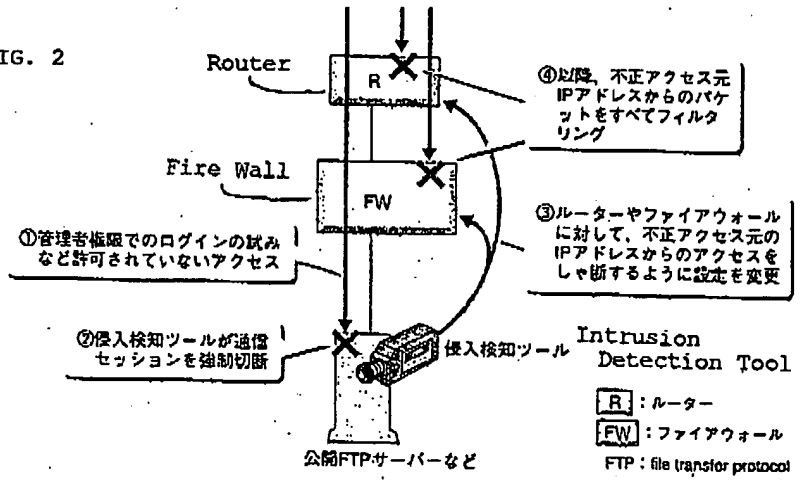
不正アクセスの検知など，CyberCop Monitor上で発生したイベントは，共通の言葉である「ポリシー」の形でファイアウォールに通知される。ファイアウォールは，通知されたポリシーを基に，実際の設定に反映させる。ネットワークアソシエイツの菊地昭一マーケティング部ジェネラルマネージャによれば，ポリシー・ベースの連係機能は「ファイアウォール以外の製品も含めて複雑な制御を実現できる。関数ベースのAPIでは難しい」という。

ただ，ファイアウォールとの連係に対しては慎重な意見もある。不用意に設定を変更すると思わぬ穴が生じる可能性があるからだ。もちろん，同じことはルーターにも言えるが，一般には外部との防火壁としての役割を担うファイアウォールの設定ミスの方が，より深刻な被害につながる。

そもそもファイアウォールやルーターは基本的に，不要なポートは閉じ，外部からのアクセスは禁止しておくべきもの。インターネット側からの不正アクセスに対して，頻繁にフィルタリング設定を変更する必要がある場合は，

図2 ルーターやファイアウォールとの連係機能を使えば，特定IPアドレスからの通信をしゃ断できる 実際に不正アクセスをしゃ断するまでのプロセスは，①から④の流れで進む。

FIG. 2



Citation 1

OPSEC＝open platform for secure enterprise connectivity。イスラエルのチェック・ポイント・ソフトウエア・テクノロジーズのファイアウォール製品「FireWall-1」と組み合わせて使えるようにするためのAPI（application programming interface）。ワクチン・ソフト，URLフィルタリング・ソフトなどにも対応製品がある。

設定自体を見直した方がよい。

ただ，最近では社内の部門ごとにファイアウォールを設置するようなケースも徐々に増えている。こうした社内のファイアウォールやルーターに対しては，連係機能は有効と言えそうだ。

存在を隠せるステルス・モード

侵入検知ツールを利用していることがクラッカに知られると，ツールそのものが攻撃対象になる可能性がある。このため，多くのネットワーク監視型ツールでは，「ステルス・モード」と呼ばれる機能がある（図3）。

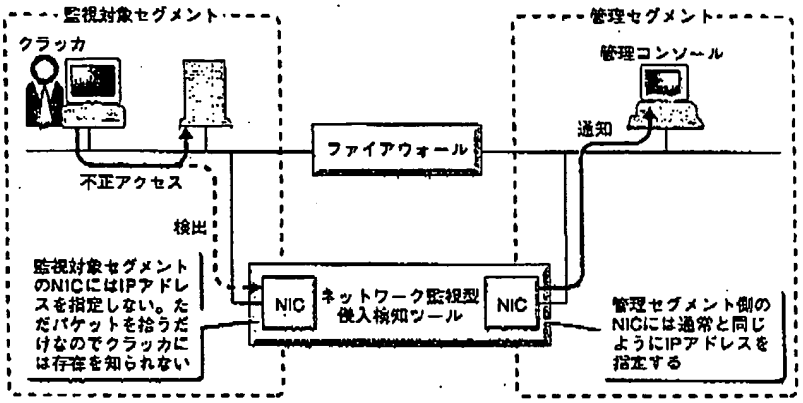
具体的には，ツールを走らせるマシンに2枚のNICを差し，1枚のNICにはIPアドレスを指定しないで監視対象セグメント側につなぐ。こうすることで監視対象セグメント側のNICは，一切パケットを送信しないデータ収集用のプローブ（探り針）として利用でき，ツールの存在を隠せる。

ステルス・モードは通常，2枚のNICを利用して一つのセグメントを監視するが，コンピュータ・アソシエイツのSessionWall-3はマシンの拡張スロットに余裕がある限り何枚でもNICを追加して複数のセグメントを同時に監視できる。

デフォルト設定では誤報の頻発も

繰り返しになるが，侵入検知ツールは万能ツールではない。不正アクセスを100パーセント検知・防御できると考えるのは間違いだ。限界や課題を見極めた上で利用する必要がある。

図3　監視対象セグメント上で「ステルス・モード」を利用すれば侵入検知ツールの存在を隠せる　多くのネットワーク監視型ツールが対応している。



NIC：network interface card

侵入検知ツールの主な問題として，①不正アクセスの誤認識，②高負荷時の取りこぼし，③LANスイッチ環境での利用，④未知の攻撃手法への対応――などがある（p.108の図4）。

まず言われるのが，①の誤認識が多いということ。例えばホスト監視型でのログインの失敗がある。仮に，一般ユーザーがIDやパスワードを1回入力間違いしただけで不正アクセスと判断するような設定だったとすると，頻繁にアラートが発生してしまう。

そのほか，例えば特定のホストとの接続性を調べるためにpingを定期的に実行している場合など，設定によっては不正アクセスと判断されてしまう可能性もある。

こうした設定の「しきい値」は，ほとんどの製品が出荷時のデフォルト設定ではかなり厳しい条件になっている場合が多いため，誤報が多く出る。ユーザーは，この状態から始めて徐々に条件を緩めていき，誤報が減るようにチューニングする必要がある。

RealSecureやNetRangerなど，数種類のテンプレートからユーザーが設定を選択できるようになっている製品もある。

100M環境，LANスイッチ使用時の問題

②の高負荷時の取りこぼしは，ほとんどのネットワーク監視型ツールが抱える課題だ（p.108の図4-b）。特に100Mイーサネットの環境では，トラフィックが多い場合に全パケットを収集/監視するのは負荷が大きい。ほとんどのベンダーはこうした状況では，「ある程度パケットを取りこぼすのは仕方がない」という。

こうした中，ネットワーク・アイスとネットワーク・アソシエイツは高負荷時のパフォーマンスに自信を見せる。両社とも100M環境でも取りこぼさないというLANアナライザを扱っており，

その技術を応用しているという。ネットワーク・アイスの「BlackICE Sentry」は100Mイーサネットでフルに負荷をかけた状態でも取りこぼしがないと，展示会などでアピールしている。

ただし，100M環境で100パーセントの検知を可能にするためにはPentiumIIの333MHz以上を採用したデュアルCPUマシンが必要，との条件付きである。

③のLANスイッチ環境での利用は，ネットワーク監視型を利用する上で最もやっかいな問題である。LANスイッチは原則として通信しているポートだけにしかフレームを流さない。つまり，特定のマシンから特定のサーバーへの通信は，ほかのポートからは見えないからである（図4-c）。

いくつかの製品はこうした問題に対応し始めている。ネットワーク・アイスの「BlackICE pro」は，ホスト監視型のように個々のマシンにネットワーク監視型ツールを分散して導入することで問題を回避できるようにした。

LANスイッチ自体にネットワーク監視型ツールを搭載する手法もある。米ODSネットワークスはISSのRealSecure N/Eを搭載したLANスイッチを出荷している。シスコ・システムズも2000年にLANスイッチにNetRangerの機能を搭載できるようにする予定である。

100パーセントの検知は無理

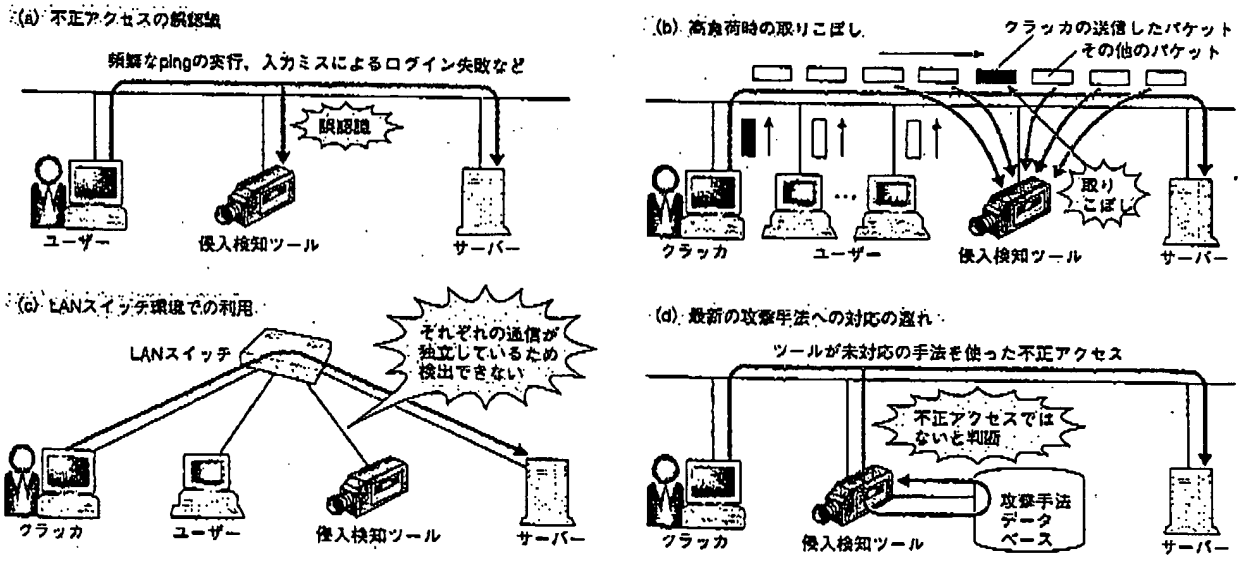
④の未知の攻撃手法への対応は，すべてのツールに共通する課題だ。OSやWWWブラウザ，アプリケーションのセキュリティ・ホールは毎日のように見つかっている。こうした新しいセキュリティ・ホールに対応するには，どうしてもタイムラグが生じてしまう。この間に攻撃を受ける可能性がある。

製品によっては，シグネチャの組み合わせなどである程度新たな攻撃手法に対応できる場合もあるが，基本的には，ベンダーによるシグネチャやルールの更新を待つ必要がある。

ネットワーク監視型の製品の中には，ユーザーが独自に監視対象を指定可能な製品がある（写真3）。こうした機能を利用すれば，公表されていてまだシグネチャが対応していない攻撃手法に自分で対処できる場合もある。

ただ，クラッカが公表されていない未知の手法を使ってくる可能性は十分ある。利用する際には，不正アクセスを100パーセント検知するのは不可能

図4 侵入検知ツールは万能ではない 侵入検知ツールを利用すればすべての不正アクセスを発見できるわけではない。一般には（a）～（d）のような問題によって誤認識したり検知できなかったりする。



Citation 1

電子メール爆弾＝メール・サーバーのダウンを狙ってクラッカが実行する不正アクセスの手法。電子メール爆撃（email bombardment）とも言う。多数かつ大容量のメールを一方的にメール・サーバーに送りつけ，メール・サーバーが処理不能に陥るまで送信し続ける。

VPN＝仮想閉域網，または仮想私設網と訳す。企業が通信事業者のサービスを利用しながら，自社で構築したネットワークと同じ使い勝手で利用できるネットワーク。

ということを常に頭に入れておく必要がある。

侵入検知ツールのそのほかの限界としては，外部と接続するルーターへの攻撃がある。侵入検知ツールにパケットが届く前であるため，基本的に対処できない。こうした外部ルーターへの攻撃は，ルーターのOSにパッチを当てるなどしか対応策はない。

また，ウイルスや☞電子メール爆弾など，パケットを見ただけでは不正アクセスかどうか判断するのが難しいものも検知するのは困難である。さらに，☞VPN（virtual private network）などを使ってパケットの中身を暗号化している場合も同様である。

写真3 監視対象をユーザーが定義可能な製品もある 写真は米アクセント・テクノロジーズの「NetProwler」で独自のURLを定義しているところ。

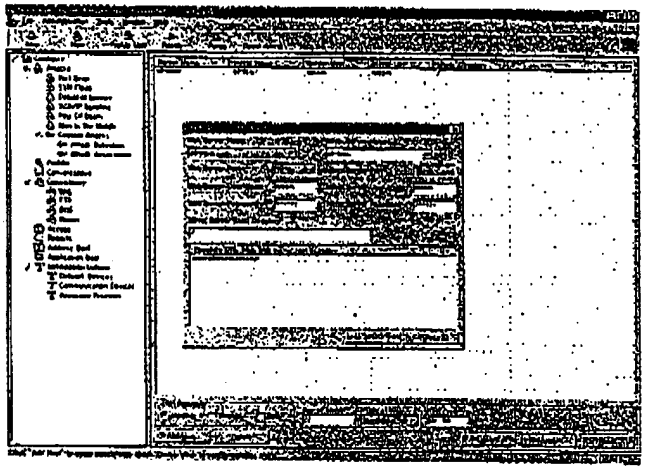
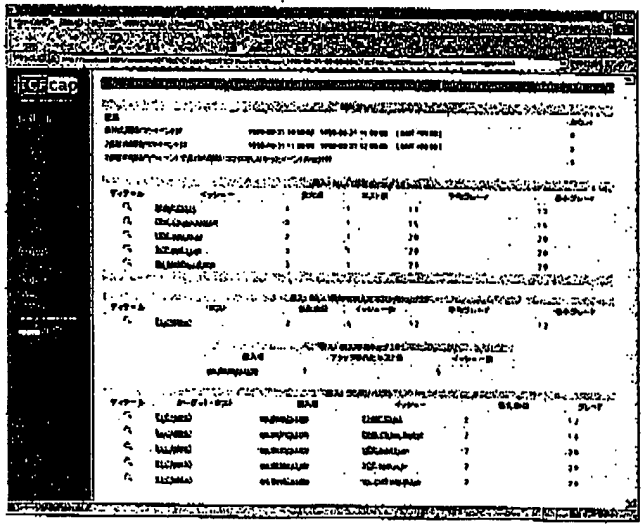


写真4 製品選択の際には，リポート機能なども確認 第三者に見せる必要がある場合には，日本語リポートの出力可否なども重要になる。写真は米ネットワーク・アイスの「BlackICE」のリポート表示画面。



シグネチャの更新頻度も大事な視点

侵入検知ツールは，いかに多くの種類の侵入手法を確実に検知できるかが製品選択の鍵になる。そういう意味で，シグネチャの更新頻度は重要だ。

逆に機能に関しては，すぐにどうしても欲しい機能でない限り，製品ごとの違いにはそれほどこだわる必要はなさそう。各ベンダーの製品とも，頻繁にバージョンアップしているため，ある時点での機能の比較はそれほど意味はないからである。

例えば，ISSのRealSecureは少し前のバージョンではURL（uniform resource locator）やファイル名など監視対象のユーザー定義ができなかったが，現行バージョンでは対応している，といった具合である。

ただ，高負荷時のパフォーマンスなどはベンダーの技術力に大きく依存する。できればユーザーの環境で実際に利用してみた方がよい。

そのほか，①設定/操作のしやすさ，②ログ表示やリポート作成機能が充実しているか――なども製品選択の基準になる（写真4）。特にリポートを第三者に見せる必要がある場合には，日本語で出力可能かどうかもチェックするとよいだろう。

さらに，今後導入を予定しているあるユーザーは，「不正アクセスを検知する性能も大事だが，サーバーやアプリケーションとの相性が重要。不安定になったり，パフォーマンスが落ちたりするようでは導入は見送る」と言う。導入する前には，こうした気配りがあってもよい。 （斉藤 栄太郎）

Citation 1

編集室から

●「空き周波数は，ぎりぎりになるまで事業者に見せない」——。ある郵政省幹部がちらりと漏らした言葉です。どの周波数帯に，どれだけの余裕があるかという情報を通信事業者や放送事業者にオープンにしてしまうと，どうしてもその空き周波数をあてにしてしまいがち。結果，周波数を有効利用しようという意識が働かず，技術開発も進まない。郵政省はそう考えているようです。

一理あります。しかし，もはや時代錯誤の感も拭えません。官が情報と資源を押さえ，市場の様子を見ながら小出しにする。こうした手法の限界は今さら指摘するまでもないはずです。NTTのアクセス網をはじめとする有線系インフラの開放はかなり進みました。今こそ，「周波数のオープン化」が必要なのではないでしょうか。 (水野)

●隣の芝生は“茶色”に見える——。今回の電波利用の取材で感じたことです。周波数の利用形態や立場ごとに帯域を増やしたい理由がそれぞれあって，“自分の帯域”は，“隣の帯域”より重要度や活用度が高いように感じているようです。話を聞くと実際，それなりの理由があってほとんどの場合，納得させられてしまいます。ただ，現実には通信や放送事業だけでなく，防災や学術目的にも使われています。いざ，立場を比べようとしても，比較の基準がなかなか見つかりません。文化の違いに優劣を付けなければならないような難しさがあります。

より効率的に電波を使うには，まずはお互いの立場や状況を正確に知ることから始める，というのが案外早道かもしれません。 (野沢)

●先日，自宅付近に落雷があり，その影響でISDNルーターが壊れました。4月に購入したばかりなので保証期間内ですが，メーカーによれば雷で壊れた場合は保証の対象外で，修理費用は1万5000円程度かかるとのこと。

パソコンを含め，ほかの電気製品は何一つ壊れていないのに，ISDNルーターだけ壊れたのに納得がいかず，このメーカーの製品だけ特に雷に弱いのでは，とも疑いました。しかしインターネットで調べてみると，私以外にもルーターやTAだけが雷で壊れたという話は結構あるようです。こうした情報が事前にわかっていれば雷対策機器を購入していた（かもしれない）のに，と悔やみました。

それにしても，メーカーは便利さだけを強調しないで，こうした情報もきちんと提供して欲しいものです。 (斉藤)

次号予告
(11月1日発行号の主な予定記事)

●特集
定額インターネットの本命
IP接続サービス，CATV，ADSL，無線LAN——。様々な定額インターネットが実現しようとしている。どのサービス，どの技術が本命か。真価に迫る。

●スペシャル・リポート
TELECOM99詳報
10月10日からスイス・ジュネーブで開催された今世紀最後の大イベントで何が起こったか。本誌取材班による独自リポート。

●ここが知りたい
iモード対応グループウエアの実用性
NTTドコモの「iモード」に対応したグループウエアやゲートウエイ製品が増えてきた。そのメリットや実用性を探る。

日経コミュニケーション
NIKKEI COMMUNICATIONS

読者の皆様へ
●乱丁・落丁本はお取り換えいたします。当社販売サービスセンターまでご連絡ください。
●本誌編集面についてのご意見・ご要望は，書面で日経コミュニケーション編集部あて〔〒102-8636 東京都千代田区平河町2-1-1，FAX (03)5210-8268，電子メール ncc@nikkeibp.co.jpにお寄せ願います。「ラウンジ」欄で採用させていただいた場合は掲載を差し上げます。掲載にあたっては編集部で誌問させていただくことがあります。また，情報提供は，編集部直通〔☎(03)5210-8270〕もご利用下さい。
●本誌掲載の広告製品・サービスについての資料請求，および本誌「新製品ラインアップ」欄で紹介された製品の資料請求には，本誌とじ込みの「資料請求カード」をご利用ください。資料請求カードはファクシミリ〔FAX (03)5210-8373〕でも受け付けています。
●当社調査部門では，よりよい誌面づくりのため，サンプリングによりアンケート方式の読者調査を恒常行っています。アンケートをお届けした場合は，なにとぞご協力のほどお願い申し上げます。

お申し込み・お問い合わせ
●本誌購読のお申し込み，あて先・電話番号の変更は日経BP社読者サービスセンター
〒134-8730 東京・葛西郵便局 私書箱20号
☎(03)5696-1111
●本誌記事に関するお問い合わせは記事案内窓口（平日10:00～12:00，13:00～16:00，☎(03)3869-8000）に電話でお願いします。

日経コミュニケーションはインターネットのWWWサーバーで情報を発信しています。ホームページのアドレス（URL）は次の通りです。
—http://www.nikkeibp.co.jp/NCC/
また，日経BP社は以下のアドレスでホームページを公開しています。
—http://www.nikkeibp.co.jp/
皆様のアクセスをお待ちしています。

発行人 竹内 正紀
編集長 前川 仏司
副編集長 井出 一仁/小山 由三/林 哲史
副編集長兼編集委員 水野 博泰/森川 雅男
編集 安井 晴海/朱田 正明/白川 佳三
川崎 哲介/野沢 哲生/中川 ヒロミ
高田 学也/塩沢 善雄/吉野 次郎
斉藤 栄太郎/高堰 芳/半沢 智
鳥海 忠承
広告長 岡本 明
広告課長 中村 了
広告 佐谷 裕之/佐藤 明裕/森田 隆介
中田 知之/佐々木 誠一/中原 伸也
尾関 敬一郎
販売部次長 池田 竜矢
販売 宮井 清孝
デザイン エステム
制作 ポリセント/日経BPクリエーティブ

翻訳権特約誌
Data Communications (CMP Media Inc.)

 ISSN 0910-7215

日経BP社
Nikkei Business Publications, Inc.
東京都千代田区平河町2-7-6 〒102-8622

日本ABC協会加盟誌
(新聞雑誌部数公査機構)

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.